#3

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

ATTY. DOCKET NO. 040373-0263

In re Patent Application of
Koji MANABE
Serial No. Unassigned
Filed: September 24, 1999
For: WORKS PROTECTING SYSTEM AND WORKS PROTECTING METHOD THEREFOR

CLAIM FOR CONVENTION PRIORITY

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

The benefit of the filing date of the following prior foreign application filed in the following foreign country is hereby requested, and the right of priority provided in 35 U.S.C. 119, is hereby claimed.

In support of this claim, filed herewith is a certified copy of said original foreign application:

Japanese Patent Application
No. 10-278153 filed September 30, 1998.

Respectfully submitted,

September 24, 1999
Date

Ronald Corbett 36,489
for David A. Blumenthal
Reg. No. 26,257

FOLEY & LARDNER
3000 K Street, N.W., Suite 500
Washington, D.C. 20007-5109
Tel: (202) 672-5300

US

日 本 国 特 許 庁

PATENT OFFICE
JAPANESE GOVERNMENT

Manabe
040373/0963

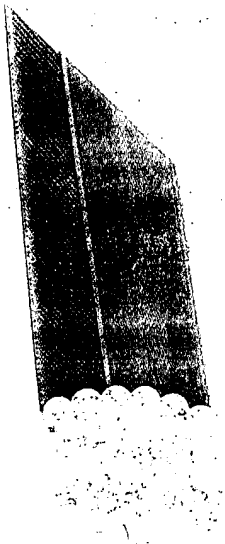
別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: １９９８年　９月３０日

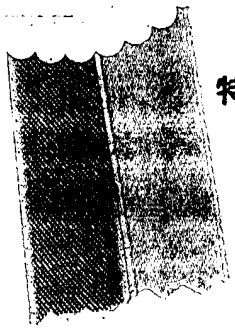
出願番号
Application Number: 平成１０年特許願第２７８１５３号

出願人
Applicant (s): 日本電気株式会社



CERTIFIED COPY OF
PRIORITY DOCUMENT

１９９９年　４月　２日



特許庁長官
Commissioner,
Patent Office 伊佐山建志

出証番号　出証特平１１－３０１９９７８

【書類名】　特許願

【整理番号】　68501622

【提出日】　平成10年 9月30日

【あて先】　特許庁長官　　殿

【国際特許分類】　G06F 9/06

G06F 12/14

【発明の名称】　著作物保護システムおよびその著作物保護方法

【請求項の数】　6

【発明者】

【住所又は居所】　東京都港区芝五丁目７番１号　日本電気株式会社内

【氏名】　真鍋　浩嗣

【特許出願人】

【識別番号】　000004237

【氏名又は名称】　日本電気株式会社

【代理人】

【識別番号】　100070219

【弁理士】

【氏名又は名称】　若林　忠

【電話番号】　03-3585-1882

【選任した代理人】

【識別番号】　100100893

【弁理士】

【氏名又は名称】　渡辺　勝

【選任した代理人】

【識別番号】　100088328

【弁理士】

【氏名又は名称】　金田　暢之

【選任した代理人】

【識別番号】　100106138

【弁理士】

【氏名又は名称】　石橋　政幸

【選任した代理人】

【識別番号】　100106297

【弁理士】

【氏名又は名称】　伊藤　克博

【手数料の表示】

【予納台帳番号】　015129

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9710078

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　著作物保護システムおよびその著作物保護方法

【特許請求の範囲】

【請求項１】　著作物を伝送するＡＶデータ送信機器と、該著作物を受信する相手側の送受信機器とから構成され、

前記ＡＶデータ送信機器は、コマンド入力手段と、コマンド制御手段と、ＡＶデータ送信手段と、暗号化手段と、第１の認証手段と、第１の入出力手段と、機器ＩＤ検出手段と、認証履歴記憶手段とを備えて構成され、

前記相手側の送受信機器は、第２の入出力手段と、ＡＶデータ受信手段と、復号化手段と、第２の認証手段とを備えて構成され、

前記認証手段は、過去に認証を行った履歴がある前記相手側の送受信機器が伝送路に接続すると、お互いの機器がある規則に基づく機器であることを相互に確認する機器認証作業と、同時に前記著作物を暗号化および復号化するための暗号鍵を共有する鍵交換作業とを行う手段である著作物保護システム。

【請求項２】　著作物を伝送するＡＶデータ送信機器と、該著作物を受信する複数の相手側の送受信機器とから構成され、

前記ＡＶデータ送信機器は、コマンド入力手段と、コマンド制御手段と、ＡＶデータ送信手段と、暗号化手段と、第１の認証手段と、第１の入出力手段と、機器ＩＤ検出手段と、認証履歴記憶手段と、暗号鍵記憶手段とを備えて構成され、

前記複数の相手側の送受信機器は、それぞれ第２の入出力手段と、ＡＶデータ受信手段と、復号化手段と、第２の認証手段とを備えて構成され、

前記認証手段は、過去に認証を行った履歴がある前記相手側の送受信機器が伝送路に接続すると、お互いの機器がある規則に基づく機器であることを相互に確認する機器認証作業と、同時に前記著作物を暗号化および復号化するための暗号鍵を共有する鍵交換作業とを行う手段である著作物保護システム。

【請求項３】　著作物を伝送するＡＶデータ送信機器と、該著作物を受信する相手側の送受信機器とから構成され、

前記ＡＶデータ送信機器は、コマンド入力手段と、コマンド制御手段と、ＡＶデータ送信手段と、暗号化手段と、第１の認証手段と、第１の入出力手段と、機

器ＩＤ検出手段とを備えて構成され、

前記相手側の送受信機器は、第２の入出力手段と、ＡＶデータ受信手段と、復号化手段と、第２の認証手段とを備えて構成され、

前記認証手段は、前記相手側の送受信機器が伝送路に接続すると、お互いの機器がある規則に基づく機器であることを相互に確認する機器認証作業と、同時に前記著作物を暗号化および復号化するための暗号鍵を共有する鍵交換作業とを行う手段である著作物保護システム。

【請求項４】　前記機器ＩＤ検出手段により、前記相手側の送受信機器ＩＤを検出する段階と、

前記認証履歴記憶手段が記憶している履歴情報の中に前記相手側の送受信機器ＩＤが含まれているかどうかを調べる段階と、

前記履歴情報の中に前記相手側の送受信機器ＩＤが含まれている場合、前記第１の認証手段により、相手側の前記第２の認証手段と前記機器認証作業と前記鍵交換作業とを行う段階と、

その後、前記コマンド入力手段に対してユーザからＡＶデータ送信指示のコマンド入力があると、前記コマンド制御手段を介して前記ＡＶデータ送信手段に前記コマンドが通知され、前記ＡＶデータ送信手段により、前記ＡＶデータの送信を開始する段階と、

前記履歴情報の中に前記相手側の送受信機器ＩＤが含まれていない場合、前記コマンド入力手段に対してユーザからＡＶデータ送信指示のコマンド入力が来るのを待つ段階と、

該ＡＶデータ送信指示のコマンド入力があると、前記第１の認証手段により、相手側の前記第２の認証手段と前記機器認証作業と前記鍵交換作業とを行う段階と、

前記機器認証作業と前記鍵交換作業とを終えると、前記認証履歴記憶手段に前記相手側の送受信機器ＩＤを履歴情報として記録する段階と、

前記コマンド制御手段を介して前記ＡＶデータ送信手段に前記コマンドが通知され、前記ＡＶデータ送信手段により、前記ＡＶデータの送信を開始する段階と、

前記暗号化手段により、前記ＡＶデータを前記暗号鍵を用いて暗号化し、前記第１の入出力手段へ送出する段階と、

該第１の入出力手段により、前記暗号化されたＡＶデータを伝送路に送出する段階と、

前記第２の入出力手段により、前記暗号化されたＡＶデータを前記伝送路から受け取る段階と、

前記復号化手段により、前記暗号化されたＡＶデータを前記暗号鍵を用いて復号化し、前記ＡＶデータ受信手段へ送出する段階と、

該ＡＶデータ受信手段により、前記復号化されたＡＶデータを受け取る段階とを有する請求項１に記載の著作物保護システムの著作物保護方法。

【請求項５】　前記機器ＩＤ検出手段により、第１の相手側の送受信機器ＩＤを検出する段階と、

前記認証履歴記憶手段が記憶している履歴情報の中に前記第１の相手側の送受信機器ＩＤが含まれているかどうかを調べる段階と、

前記履歴情報の中に前記第１の相手側の送受信機器ＩＤが含まれている場合、前記第１の認証手段により、第１の相手側の前記第２の認証手段と前記機器認証作業と前記鍵交換作業とを行う段階と、

前記鍵交換作業の結果、共有した暗号鍵を第１の暗号鍵として暗号鍵記憶手段に記録する段階と、

前記機器ＩＤ検出手段により、第２の相手側の送受信機器ＩＤを検出する段階と、

前記認証履歴記憶手段が記憶している履歴情報の中に前記第２の相手側の送受信機器ＩＤが含まれているかどうかを調べる段階と、

前記履歴情報の中に前記第２の相手側の送受信機器ＩＤが含まれている場合、前記第１の認証手段により、第２の相手側の前記第２の認証手段と前記機器認証作業と前記鍵交換作業とを行う段階と、

前記鍵交換作業の結果、共有した暗号鍵を第２の暗号鍵として暗号鍵記憶手段に記録する段階と、

その後、前記コマンド入力手段に対してユーザから前記第１の相手側の送受信

機器または前記第２の相手側の送受信機器に対してのＡＶデータ送信指示のコマンド入力があると、前記コマンド制御手段を介して前記ＡＶデータ送信手段に前記コマンドが通知され、前記ＡＶデータ送信手段により、前記ＡＶデータの送信を開始する段階と、

前記履歴情報の中に前記第１の相手側の送受信機器ＩＤが含まれていない場合、

前記コマンド入力手段に対してユーザから前記第１の相手側の送受信機器に対してのＡＶデータ送信指示のコマンド入力が来るのを待つ段階と、

該ＡＶデータ送信指示のコマンド入力があると、前記第１の認証手段により、前記第１の相手側の前記第２の認証手段と前記機器認証作業と前記鍵交換作業とを行う段階と、

前記機器認証作業と前記鍵交換作業とを終えると、前記認証履歴記憶手段に前記第１の相手側の送受信機器ＩＤを履歴情報として記録する段階と、

前記鍵交換作業の結果、共有した暗号鍵を第１の暗号鍵として暗号鍵記憶手段に記録する段階と、

前記履歴情報の中に前記第２の相手側の送受信機器ＩＤが含まれていない場合、

前記コマンド入力手段に対してユーザから前記第２の相手側の送受信機器に対してのＡＶデータ送信指示のコマンド入力が来るのを待つ段階と、

該ＡＶデータ送信指示のコマンド入力があると、前記第１の認証手段により、前記第２の相手側の前記第２の認証手段と前記機器認証作業と前記鍵交換作業とを行う段階と、

前記機器認証作業と前記鍵交換作業とを終えると、前記認証履歴記憶手段に前記第２の相手側の送受信機器ＩＤを履歴情報として記録する段階と、

前記鍵交換作業の結果、共有した暗号鍵を第２の暗号鍵として暗号鍵記憶手段に記録する段階と、

前記コマンド制御手段を介して前記ＡＶデータ送信手段に前記コマンドが通知され、前記ＡＶデータ送信手段により、前記第１の相手側の送受信機器または前記第２の相手側の送受信機器に対してのＡＶデータの送信を開始する段階と、

前記コマンド入力手段に対してユーザから前記第１の相手側の送受信機器に対してのＡＶデータ送信指示のコマンド入力がある場合は、

前記暗号化手段により、前記ＡＶデータを前記第１の暗号鍵を用いて暗号化し、前記第１の入出力手段へ送出する段階と、

該第１の入出力手段により、前記暗号化されたＡＶデータを伝送路に送出する段階と、

前記第１の相手側の第２の入出力手段により、前記暗号化されたＡＶデータを前記伝送路から受け取る段階と、

前記第１の相手側の復号化手段により、前記暗号化されたＡＶデータを前記第１の暗号鍵を用いて復号化し、前記第１の相手側のＡＶデータ受信手段へ送出する段階と、

該ＡＶデータ受信手段により、前記復号化されたＡＶデータを受け取る段階と、

前記コマンド入力手段に対してユーザから前記第２の相手側の送受信機器に対してのＡＶデータ送信指示のコマンド入力がある場合は、

前記暗号化手段により、前記ＡＶデータを前記第２の暗号鍵を用いて暗号化し、前記第１の入出力手段へ送出する段階と、

該第１の入出力手段により、前記暗号化されたＡＶデータを伝送路に送出する段階と、

前記第２の相手側の第２の入出力手段により、前記暗号化されたＡＶデータを前記伝送路から受け取る段階と、

前記第２の相手側の復号化手段により、前記暗号化されたＡＶデータを前記第２の暗号鍵を用いて復号化し、前記第２の相手側のＡＶデータ受信手段へ送出する段階と、

該ＡＶデータ受信手段により、前記復号化されたＡＶデータを受け取る段階とを有する請求項２に記載の著作物保護システムの著作物保護方法。

【請求項６】　前記ＡＶデータの伝送路はＩＥＥＥ１３９４高速シリアルバスである請求項４または請求項５に記載の著作物保護システムの著作物保護方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、ＡＶデータを送受信する際の機器間の著作物保護システム及びその著作物保護方法に関する。

【０００２】

【従来の技術】

従来、ユーザにアナログデータとして扱われてきたＡＶデータが、近年、デジタル衛星放送、インターネット配信、ＤＶＤなどの普及によってデジタルデータのまま扱われるようになった。またデジタルデータを高速に伝送できるIEEE１３９４高速シリアルバスが実用化されるに至り、著作権保護の観点からＡＶデータを送受信する際の機器間の著作物保護システムが提案されている。

【０００３】

例えば、日経エレクトロニクス１９９８．３．２３ｐｐ．４７－５３「ＩＥＥＥ１３９４のコピー防止技術、公開鍵/共通鍵併用で一本化」には認証手段および暗号化手段を備える著作物保護システムが示されている。そのシステムのブロック図を図４に示し、状態遷移図を図５に示す。この従来の著作物保護システムのの構成は次の通りである。コマンド入力手段１１に対してユーザからＡＶデータ送信指示があると（Ｓ１１）、コマンド制御手段２１を介して認証手段５１は相手側の認証手段１４１と認証を行う（Ｓ１２）。認証を終えると、ＡＶデータ送信手段３１はＡＶデータの送信を開始する（Ｓ１３）。ＡＶデータは暗号化手段４１において暗号鍵を用いて暗号化され入出力手段６１を介して伝送路に送出される。相手側の送受信機器において、入出力手段１１１は伝送路から暗号化されたＡＶデータを受け取る。復号化手段１３１は暗号化されたＡＶデータを暗号鍵を用いて復号し、ＡＶデータ受信手段１２１は復号化されたＡＶデータを受け取る。

【０００４】

【発明が解決しようとする課題】

上述の説明で明らかなように、従来の著作物保護システムはユーザからＡＶデ

ータ伝送指示があってはじめて相手側の送受信機器と認証を行うため、ＡＶデータを伝送するまでに時間がかかるという問題があった。

【０００５】

上述の従来技術の問題点に鑑み、本発明の目的は、ＡＶデータ伝送指示からＡＶデータを伝送するまでの時間を短縮する著作物保護システム及びその著作物保護方法を提供することにある。

【０００６】

【課題を解決するための手段】

本発明の著作物保護システムは、

著作物を伝送するＡＶデータ送信機器と、著作物を受信する相手側の送受信機器とから構成され、ＡＶデータ送信機器は、コマンド入力手段と、コマンド制御手段と、ＡＶデータ送信手段と、暗号化手段と、第１の認証手段と、第１の入出力手段と、機器ＩＤ検出手段と、認証履歴記憶手段とを備えて構成され、相手側の送受信機器は、第２の入出力手段と、ＡＶデータ受信手段と、復号化手段と、第２の認証手段とを備えて構成され、認証手段は、過去に認証を行った履歴がある相手側の送受信機器が伝送路に接続すると、お互いの機器がある規則に基づく機器であることを相互に確認する機器認証作業と、同時に著作物を暗号化および復号化するための暗号鍵を共有する鍵交換作業とを行う手段である。

【０００７】

また、著作物を伝送するＡＶデータ送信機器と、著作物を受信する複数の相手側の送受信機器とから構成され、ＡＶデータ送信機器は、コマンド入力手段と、コマンド制御手段と、ＡＶデータ送信手段と、暗号化手段と、第１の認証手段と、第１の入出力手段と、機器ＩＤ検出手段と、認証履歴記憶手段と、暗号鍵記憶手段とを備えて構成され、複数の相手側の送受信機器は、それぞれ第２の入出力手段と、ＡＶデータ受信手段と、復号化手段と、第２の認証手段とを備えて構成され、認証手段は、過去に認証を行った履歴がある相手側の送受信機器が伝送路に接続すると、お互いの機器がある規則に基づく機器であることを相互に確認する機器認証作業と、同時に著作物を暗号化および復号化するための暗号鍵を共有する鍵交換作業とを行う手段であってもよい。

【０００８】

また、著作物を伝送するＡＶデータ送信機器と、著作物を受信する相手側の送受信機器とから構成され、ＡＶデータ送信機器は、コマンド入力手段と、コマンド制御手段と、ＡＶデータ送信手段と、暗号化手段と、第１の認証手段と、第１の入出力手段と、機器ＩＤ検出手段とを備えて構成され、相手側の送受信機器は、第２の入出力手段と、ＡＶデータ受信手段と、復号化手段と、第２の認証手段とを備えて構成され、認証手段は、相手側の送受信機器が伝送路に接続すると、お互いの機器がある規則に基づく機器であることを相互に確認する機器認証作業と、同時に前記著作物を暗号化および復号化するための暗号鍵を共有する鍵交換作業とを行う手段であってもよい。

【０００９】

本発明の著作物保護システムの著作物保護方法は、

機器ＩＤ検出手段により、相手側の送受信機器ＩＤを検出する段階と、認証履歴記憶手段が記憶している履歴情報の中に相手側の送受信機器ＩＤが含まれているかどうかを調べる段階と、履歴情報の中に相手側の送受信機器ＩＤが含まれている場合、第１の認証手段により、相手側の第２の認証手段と機器認証作業と鍵交換作業とを行う段階と、その後、コマンド入力手段に対してユーザからＡＶデータ送信指示のコマンド入力があると、コマンド制御手段を介してＡＶデータ送信手段にコマンドが通知され、ＡＶデータ送信手段により、ＡＶデータの送信を開始する段階と、履歴情報の中に相手側の送受信機器ＩＤが含まれていない場合、コマンド入力手段に対してユーザからＡＶデータ送信指示のコマンド入力が来るのを待つ段階と、ＡＶデータ送信指示のコマンド入力があると、第１の認証手段により、相手側の第２の認証手段と機器認証作業と鍵交換作業とを行う段階と、機器認証作業と鍵交換作業とを終えると、認証履歴記憶手段に相手側の送受信機器ＩＤを履歴情報として記録する段階と、コマンド制御手段を介してＡＶデータ送信手段にコマンドが通知され、ＡＶデータ送信手段により、ＡＶデータの送信を開始する段階と、暗号化手段により、ＡＶデータを暗号鍵を用いて暗号化し、第１の入出力手段へ送出する段階と、第１の入出力手段により、暗号化されたＡＶデータを伝送路に送出する段階と、第２の入出力手段により、暗号化された

ＡＶデータを伝送路から受け取る段階と、復号化手段により、暗号化されたＡＶデータを暗号鍵を用いて復号化し、ＡＶデータ受信手段へ送出する段階と、ＡＶデータ受信手段により、復号化されたＡＶデータを受け取る段階とを有する。

【００１０】

また、機器ＩＤ検出手段により、第１の相手側の送受信機器ＩＤを検出する段階と、認証履歴記憶手段が記憶している履歴情報の中に第１の相手側の送受信機器ＩＤが含まれているかどうかを調べる段階と、履歴情報の中に第１の相手側の送受信機器ＩＤが含まれている場合、第１の認証手段により、第１の相手側の第２の認証手段と機器認証作業と鍵交換作業とを行う段階と、鍵交換作業の結果、共有した暗号鍵を第１の暗号鍵として暗号鍵記憶手段に記録する段階と、機器ＩＤ検出手段により、第２の相手側の送受信機器ＩＤを検出する段階と、認証履歴記憶手段が記憶している履歴情報の中に第２の相手側の送受信機器ＩＤが含まれているかどうかを調べる段階と、履歴情報の中に第２の相手側の送受信機器ＩＤが含まれている場合、前記第１の認証手段により、第２の相手側の前記第２の認証手段と機器認証作業と鍵交換作業とを行う段階と、鍵交換作業の結果、共有した暗号鍵を第２の暗号鍵として暗号鍵記憶手段に記録する段階と、その後、コマンド入力手段に対してユーザから第１の相手側の送受信機器または第２の相手側の送受信機器に対してのＡＶデータ送信指示のコマンド入力があると、コマンド制御手段を介してＡＶデータ送信手段にコマンドが通知され、ＡＶデータ送信手段により、ＡＶデータの送信を開始する段階と、履歴情報の中に第１の相手側の送受信機器ＩＤが含まれていない場合、コマンド入力手段に対してユーザから第１の相手側の送受信機器に対してのＡＶデータ送信指示のコマンド入力が来るのを待つ段階と、ＡＶデータ送信指示のコマンド入力があると、第１の認証手段により、第１の相手側の第２の認証手段と機器認証作業と鍵交換作業とを行う段階と、機器認証作業と鍵交換作業とを終えると、認証履歴記憶手段に第１の相手側の送受信機器ＩＤを履歴情報として記録する段階と、鍵交換作業の結果、共有した暗号鍵を第１の暗号鍵として暗号鍵記憶手段に記録する段階と、履歴情報の中に第２の相手側の送受信機器ＩＤが含まれていない場合、コマンド入力手段に対してユーザから第２の相手側の送受信機器に対してのＡＶデータ送信指示のコマ

ンド入力が来るのを待つ段階と、ＡＶデータ送信指示のコマンド入力があると、第１の認証手段により、第２の相手側の第２の認証手段と機器認証作業と鍵交換作業とを行う段階と、機器認証作業と鍵交換作業とを終えると、認証履歴記憶手段に第２の相手側の送受信機器ＩＤを履歴情報として記録する段階と、鍵交換作業の結果、共有した暗号鍵を第２の暗号鍵として暗号鍵記憶手段に記録する段階と、コマンド制御手段を介してＡＶデータ送信手段にコマンドが通知され、ＡＶデータ送信手段により、第１の相手側の送受信機器または第２の相手側の送受信機器に対してのＡＶデータの送信を開始する段階と、コマンド入力手段に対してユーザから第１の相手側の送受信機器に対してのＡＶデータ送信指示のコマンド入力がある場合は、暗号化手段により、ＡＶデータを第１の暗号鍵を用いて暗号化し、第１の入出力手段へ送出する段階と、第１の入出力手段により、暗号化されたＡＶデータを伝送路に送出する段階と、第１の相手側の第２の入出力手段により、暗号化されたＡＶデータを伝送路から受け取る段階と、第１の相手側の復号化手段により、暗号化されたＡＶデータを第１の暗号鍵を用いて復号化し、第１の相手側のＡＶデータ受信手段へ送出する段階と、ＡＶデータ受信手段により、復号化されたＡＶデータを受け取る段階と、コマンド入力手段に対してユーザから第２の相手側の送受信機器に対してのＡＶデータ送信指示のコマンド入力がある場合は、暗号化手段により、ＡＶデータを第２の暗号鍵を用いて暗号化し、第１の入出力手段へ送出する段階と、第１の入出力手段により、暗号化されたＡＶデータを伝送路に送出する段階と、第２の相手側の第２の入出力手段により、暗号化されたＡＶデータを伝送路から受け取る段階と、第２の相手側の復号化手段により、暗号化されたＡＶデータを第２の暗号鍵を用いて復号化し、第２の相手側のＡＶデータ受信手段へ送出する段階と、ＡＶデータ受信手段により、復号化されたＡＶデータを受け取る段階とを有してもよい。

【００１１】

また、ＡＶデータの伝送路はＩＥＥＥ１３９４高速シリアルバスであってもよい。

【００１２】

本発明の著作物保護システムおよびその著作物保護方法は、過去に認証を行っ

た履歴がある送受信機器が伝送路に接続すると、機器認証および鍵交換を行うことを特徴とするものであり、ユーザからのコマンド入力時点から著作物伝送開始までの時間を従来に比較して大幅に短縮するものである。

【００１３】

機器ＩＤ検出手段は相手側の送受信機器が伝送路に接続すると、入出力手段を介して、その機器ＩＤを検出する。ここで伝送路としては、例えば、ＩＥＥＥ１３９４高速シリアルバスを使うことが可能であり、また、相手側の送受信機器とは、例えば、入出力手段、ＡＶデータ受信手段、復号化手段、認証手段を備えて構成される著作物の送受信機器である。機器ＩＤ検出手段が相手側の送受信機器の機器ＩＤを検出すると、認証履歴記憶手段が記憶している履歴情報の中にその機器ＩＤが含まれているかどうかを調べる。

【００１４】

もし、履歴情報の中にその機器ＩＤが含まれている場合、認証手段は相手側の認証手段と認証を行う。ここで認証とは、お互いの機器がある規則に基づく機器であることを相互に確認する機器認証作業であり、また、同時に著作物を暗号化および復号化するための暗号鍵を共有する鍵交換作業である。その後いつでも、コマンド入力手段に対してユーザからＡＶデータ送信指示があると、コマンド制御手段を介してＡＶデータ送信手段にそのコマンドが通知され、ＡＶデータ送信手段はＡＶデータの送信を開始する。ＡＶデータは暗号化手段において暗号鍵を用いて暗号化され入出力手段を介してＩＥＥＥ１３９４高速シリアルバスなどの伝送路に送出される。相手側の送受信機器において、入出力手段はＩＥＥＥ１３９４高速シリアルバスなどの伝送路から暗号化されたＡＶデータを受け取る。復号化手段は暗号化されたＡＶデータを暗号鍵を用いて復号し、ＡＶデータ受信手段は復号化されたＡＶデータを受け取る。

【００１５】

もし履歴情報の中に機器ＩＤが含まれていない場合、コマンド入力手段に対してユーザからＡＶデータ送信指示が来るのを待つ。ＡＶデータ送信指示があると、認証手段は相手側の認証手段と認証を行う。認証を終えると、認証履歴記憶手段に相手側の機器ＩＤを履歴情報として記録する。ＡＶデータ送信手段はＡＶデ

ータの送信を開始する。ＡＶデータは暗号化手段において暗号鍵を用いて暗号化され入出力手段を介して伝送路に送出される。相手側の送受信機器において、入出力手段は伝送路から暗号化されたＡＶデータを受け取る。復号化手段は暗号化されたＡＶデータを暗号鍵を用いて復号し、ＡＶデータ受信手段は復号化されたＡＶデータを受け取る。

【００１６】

【発明の実施の形態】

（本発明の第１の実施の形態）

図１は本発明の第１の実施の形態の著作物保護システムの構成を示すブロック図である。図１を参照すると、機器ＩＤ検出手段７０は相手側の送受信機器が伝送路に接続すると、入出力手段６０を介して、その機器ＩＤを検出する。ここで伝送路としては、例えば、ＩＥＥＥ１３９４高速シリアルバスが好適である。また、相手側の送受信機器とは、例えば、入出力手段１１０、ＡＶデータ受信手段１２０、復号化手段１３０、認証手段１４０を備えて構成される著作物の送受信機器であり、具体的には、デジタルテレビ受像機、書き込み可能なＤＶＤ装置すなわちＤＶＤ－ＲＡＭ、デジタル方式のＶＴＲすなわちＤ－ＶＨＳなどが好適である。機器ＩＤ検出手段７０が相手側の送受信機器の機器ＩＤを検出すると、認証履歴記憶手段８０が記憶している履歴情報の中にその機器ＩＤが含まれているかどうかを調べる。もし、履歴情報の中にその機器ＩＤが含まれている場合、認証手段５０は相手側の認証手段１４０と認証を行う。

【００１７】

ここで認証とは、お互いの機器がある規則に基づく機器であることを相互に確認する機器認証作業と、同時に著作物を暗号化および復号化するための暗号鍵を共有する鍵交換作業とからなる。認証のためのデジタル署名方式および鍵配送方式はこれまで考案されている様々な方式を用いることが可能であるが、楕円ＤＳＡ(Digital Signature Algorithm)署名および楕円ＤＨ(Diffie-Hellman)鍵配送を用いることが好適である。楕円ＤＳＡ署名(以下EC-DSAという)について以下に述べる。EC-DSAはANSI X9.62などに規定されており、その内容は、鍵生成、署名生成、署名照合の三つの段階からなる。

【００１８】

まず、鍵生成の手順は次の通りである。

【００１９】

(1) EC-DSA鍵生成

デバイスＡにおいて

１．ＺＰ上に構成する楕円曲線Ｅを選択する。E(ZP)上の点の数は大きな素数ｎで割り切れること。

２．位数ｎの点Ｐ∈E(ZP)を選択する。

３．区間［１，ｎ－１］のなかから静的に特有かつ予言できない整数ｄを選択する。

４．Ｑ＝ｄＰを計算する。

５．Ａの公開鍵は（Ｅ，Ｐ，ｎ，Ｑ）、Ａの秘密鍵はｄとする。

【００２０】

つぎに、署名生成手順は以下の通りである。

【００２１】

(2) EC-DSA署名生成

デバイスＡにおいて、以下のようにメッセージｍを暗号化する。

１．区間［１，ｎ－１］のなかから静的に特有かつ予言できない整数ｋを選択する。

２．ｋＰ＝（ｘ１，ｙ１）およびｒ＝ｘ１ ｍｏｄ ｎを計算する。ここでｘ１はたとえばバイナリ表現からの変換によって一つの整数と見なされる。もしｒ＝０ならばステップ１に戻る（セキュリティ上の理由である。ｒ＝０なら暗号等式ｓ＝ｋ－１{ｈ（ｍ）＋ｄｒ} ｍｏｄ ｎ が秘密鍵ｄを含まないためである。）。

３．ｋ－１ ｍｏｄ ｎ を計算する。

４．ｓ＝ｋ－１{ｈ（ｍ）＋ｄｒ} ｍｏｄ ｎを計算する。ここでｈはセキュアハッシュアルゴリズム（SHA-1）である。

５．もしｓ＝０ならばステップ１に戻る（もしｓ＝０ならば、ｓ－１ ｍｏｄ ｎが存在しない。；ｓ－１は署名照合のステップ２で必要である。）。

６．メッセージｍの署名を整数の組み（ｒ，ｓ）とする。

【００２２】

さらに署名照合の手順は以下の通りである。

【００２３】

(3) EC-DSA署名照合

ｍのなかのデバイスＡの署名（ｒ，ｓ）を照合するために、デバイスＢは以下のことを行う。

１．Ａの公開鍵（Ｅ，Ｐ，ｎ，Ｑ）の真のコピーを得る。

２．ｒおよびｓが区間［１，ｎ－１］の整数であることを照合する。

３．ｗ＝ｓ－１ ｍｏｄ ｎおよびｈ（ｍ）を計算する。

４．ｕ１＝ｈ（ｍ）ｗ ｍｏｄ ｎおよびｕ２＝ｒｗ ｍｏｄ ｎを計算する。

５．ｕ１Ｐ＋ｕ２Ｑ＝（ｘ０，ｙ０）およびｖ＝ｘ０ ｍｏｄ ｎを計算する。

６．ｖ＝ｒならば署名を認める。

【００２４】

つぎに楕円ＤＨ鍵配送(以下EC-DHという)について述べる。ＥＣ－ＤＨはANSI X9.63などに規定されており、その内容は鍵生成および交換と鍵共有の二つの段階からなる。

【００２５】

まず、鍵生成および交換の手順は以下の通りである。

【００２６】

(1) EC-DH鍵生成および交換

デバイスＡにおいて

１．区間［２，ｎ－２］のなかから静的に特有かつ予言できない整数ｘを選択する。

２．ａ＝ｘＰを計算する。

３．デバイスＡはデバイスＢにａを送る。

【００２７】

デバイスＢにおいて

１．区間［２，ｎ－２］のなかから静的に特有かつ予言できない整数ｙを選択す

る。

２．ｂ＝ｙＰを計算する。

1.デバイスＢはデバイスＡにｂを送る。

【００２８】

次に鍵共有の手順を以下に述べる。

【００２９】

（２）EC-DH鍵共有

１．デバイスＡにおいてＫＡ＝ｘｂ＝ｘｙＰにより共通鍵を生成する。

２．デバイスＢにおいてＫＢ＝ｘａ＝ｘｙＰにより共通鍵を生成する。

３．ＫＡ＝ＫＢなのでデバイスＡとデバイスＢは鍵を共有する。

【００３０】

認証を終えると、その後いつでも、コマンド入力手段１０に対してユーザからＡＶデータ送信指示があると、コマンド制御手段２０を介してＡＶデータ送信手段３０にそのコマンドが通知され、ＡＶデータ送信手段３０はＡＶデータの送信を開始する。コマンド入力手段としては、例えば、キーボードやマウス、リモコンなどが好適である。ＡＶデータとしては、様々なフォーマットのＡＶデータを扱うことが可能であり、ＭＰＥＧ２規格に準じて圧縮されたトランスポートストリームが好適である。ＡＶデータ送信手段３０とは、例えばデジタル衛星放送受信装置、インターネットからのＡＶデータ受信装置、ＤＶＤ装置などが好適である。ＡＶデータは暗号化手段４０において暗号鍵を用いて暗号化され入出力手段６０を介してＩＥＥＥ１３９４高速シリアルバスなどの伝送路に送出される。

【００３１】

暗号化手段で用いいる暗号方式としては、これまでに考案されている様々なブロック暗号を用いることが可能である。例えば、ブロウフィッシュ暗号が好適である。相手側の送受信機器において、入出力手段１１０はＩＥＥＥ１３９４高速シリアルバスなどの伝送路から暗号化されたＡＶデータを受け取る。復号化手段１３０は暗号化されたＡＶデータを暗号鍵を用いて復号し、ＡＶデータ受信手段１２０は復号化されたＡＶデータを受け取る。ここでＡＶデータは相手側の送受信機器が、デジタルテレビ受像装置であれば必要によりＭＰＥＧ２デコード処理

を施された後表示、オーディオ出力され、また、書き込み可能なＤＶＤ装置もしくはデジタル方式のＶＴＲであれば必要なフォーマット変換の後書き込み保存される。

【００３２】

もし履歴情報の中に相手側の機器ＩＤが含まれていない場合、コマンド入力手段１０に対してユーザからＡＶデータ送信指示が来るのを待つ。コマンド入力、すなわちＡＶデータ送信指示があると、認証手段５０は相手側の認証手段１４０と認証を行う。認証を終えると、認証履歴記憶手段８０に相手側の機器ＩＤを履歴情報として記録する。ＡＶデータ送信手段３０はＡＶデータの送信を開始する。ＡＶデータは暗号化手段４０において暗号鍵を用いて暗号化され入出力手段６０を介して伝送路に送出される。相手側の送受信機器において、入出力手段１１０は伝送路から暗号化されたＡＶデータを受け取る。復号化手段１３０は暗号化されたＡＶデータを暗号鍵を用いて復号し、ＡＶデータ受信手段１２０は復号化されたＡＶデータを受け取る。

【００３３】

図２は本発明の第１の実施の形態の著作物保護システムの動作状態を示す遷移図である。図２を参照すると、機器ＩＤ検出手段７０は相手側の機器ＩＤを検出する（Ｓ１）。次に、認証履歴記憶手段８０が記憶している履歴情報の中にその機器ＩＤが含まれているかどうかを調べる（Ｓ２）。もし、履歴情報の中にその機器ＩＤが含まれている場合、認証手段５０は相手側の認証手段１４０と認証を行う（Ｓ３）。その後、コマンド入力手段１０に対してユーザからＡＶデータ送信指示があると（Ｓ４）、コマンド制御手段２０を介してＡＶデータ送信手段３０にそのコマンドが通知され、ＡＶデータ送信手段３０はＡＶデータの送信を開始する（Ｓ５）。

【００３４】

もし履歴情報の中に機器ＩＤが含まれていない場合、コマンド入力手段１０に対してユーザからＡＶデータ送信指示が来るのを待つ。ＡＶデータ送信指示があると（Ｓ６）、認証手段５０は相手側の認証手段１４０と認証を行う（Ｓ７）。認証を終えると、認証履歴記憶手段８０に相手側の機器ＩＤを履歴情報として記

録する（Ｓ８）。ＡＶデータ送信手段３０はＡＶデータの送信を開始する（Ｓ５）。

【００３５】

その後の繰り返し動作においては、認証履歴のその機器ＩＤが記録されているため、認証手段５０が認証を行い（Ｓ３）、コマンド入力手段１０に対してユーザからＡＶデータ送信指示があると（Ｓ４）、コマンド制御手段２０を介してＡＶデータ送信手段３０にそのコマンドが通知され、ＡＶデータ送信手段３０はＡＶデータの送信を開始する（Ｓ５）。

【００３６】

（本発明の第２の実施の形態）

次に、本発明の第２の実施の形態について図面を参照して詳細に説明する。

【００３７】

図３を参照すると本実施の形態は著作物伝送する相手側の送受信機器を複数備えて構成される。すなわち、機器ＩＤ検出手段７０は送受信機器が伝送路に接続すると、入出力手段６０を介して、その機器ＩＤを検出する。機器ＩＤ検出手段７０が第一の相手側の送受信機器の機器ＩＤを検出すると、認証履歴記憶手段８０が記憶している履歴情報の中にその機器ＩＤが含まれているかどうかを調べる。もし、履歴情報の中にその機器ＩＤが含まれている場合、認証手段５０は相手側の認証手段１４０と認証を行い、鍵共有の結果、暗号鍵を得る。その暗号鍵を第一の暗号鍵として暗号鍵記憶手段９０に記録する。また、機器ＩＤ検出手段７０が第二の相手側の送受信機器の機器ＩＤを検出すると、認証履歴記憶手段８０が記憶している履歴情報の中にその機器ＩＤが含まれているかどうかを調べる。もし、履歴情報の中にその機器ＩＤが含まれている場合、認証手段５０は相手側の認証手段２４０と認証を行い、鍵共有の結果、暗号鍵を得る。その暗号鍵を第二の暗号鍵として暗号鍵記憶手段９０に記録する。

【００３８】

履歴情報の中に第一の相手側の送受信機器ＩＤが含まれていない場合は、コマンド入力手段１０に対してユーザから第一の相手側の送受信機器に対してのＡＶデータ送信指示のコマンド入力が来るのを待つ。そのＡＶデータ送信指示のコマ

ンド入力があると、認証手段５０により、第一の相手側の認証手段１４０と機器認証作業と鍵交換作業とを行う。機器認証作業と鍵交換作業とを終えると、認証履歴記憶手段８０に第一の相手側の送受信機器ＩＤを履歴情報として記録する。鍵交換作業の結果、共有した暗号鍵を第一の暗号鍵として暗号鍵記憶手段９０に記録する。

【００３９】

履歴情報の中に第二の相手側の送受信機器ＩＤが含まれていない場合、コマンド入力手段１０に対してユーザから第二の相手側の送受信機器に対してのＡＶデータ送信指示のコマンド入力が来るのを待つ。そのＡＶデータ送信指示のコマンド入力があると、認証手段５０により、第二の相手側の認証手段２４０と機器認証作業と鍵交換作業とを行う。機器認証作業と鍵交換作業とを終えると、認証履歴記憶手段８０に第二の相手側の送受信機器ＩＤを履歴情報として記録する。鍵交換作業の結果、共有した暗号鍵を第二の暗号鍵として暗号鍵記憶手段９０に記録する。

【００４０】

認証および暗号鍵の記録を終えると、その後いつでも、コマンド入力手段１０に対してユーザから第一の相手側の送受信機器に対してのＡＶデータ送信指示があると、コマンド制御手段２０を介してＡＶデータ送信手段３０にそのコマンドが通知され、ＡＶデータ送信手段３０はＡＶデータの送信を開始する。ＡＶデータは暗号鍵記憶手段９０に記録されている第一の相手側の送受信機器用の暗号鍵を用いて暗号化手段４０において暗号化され入出力手段６０を介して伝送路に送出される。第一の相手側の送受信機器において、入出力手段１１０は伝送路から暗号化されたＡＶデータを受け取る。復号化手段１３０は暗号化されたＡＶデータを第一の相手側の送受信機器用の暗号鍵を用いて復号し、ＡＶデータ受信手段１２０は復号化されたＡＶデータを受け取る。

【００４１】

また、コマンド入力手段１０に対してユーザから第二の相手側の送受信機器に対してのＡＶデータ送信指示があると、コマンド制御手段２０を介してＡＶデータ送信手段３０にそのコマンドが通知され、ＡＶデータ送信手段３０はＡＶデー

タの送信を開始する。ＡＶデータは暗号鍵記憶手段９０に記録されている第二の相手側の送受信機器用の暗号鍵を用いて暗号化手段４０において暗号化され入出力手段６０を介して伝送路に送出される。第二の相手側の送受信機器において、入出力手段２１０は伝送路から暗号化されたＡＶデータを受け取る。復号化手段２３０は暗号化されたＡＶデータを第二の相手側の送受信機器用の暗号鍵を用いて復号し、ＡＶデータ受信手段２２０は復号化されたＡＶデータを受け取る。

【００４２】

本実施の形態で明らかなように本発明の著作物保護方式および装置は相手側の送受信機器が複数存在する場合においても、ユーザから著作物伝送を指示するコマンドを入力した時点から著作物伝送開始までの時間を従来に比較して大幅に短縮できる効果を有する。

【００４３】

また、ここまでの説明においては、コマンド入力手段１０ならびにコマンド制御手段２０がＡＶデータ送信機器に具備されて構成する例を示したが、コマンド入力手段１０ならびにコマンド制御手段２０はＡＶデータ送信機器に具備されないで構成することも可能である。

【００４４】

さらに、ここまでの説明においてはＡＶデータ送信機器が一つで構成する例について述べたが、本発明による効果を何ら失うことなしに、複数のＡＶデータ送信機器が存在する構成とすることも勿論可能である。

【００４５】

そして、図１および図３の実施の形態において認証履歴記憶手段８０を含まない構成とする実施の形態も本発明の別の実施の形態である。この実施の形態においては、送受信機器が伝送路に接続され、機器ＩＤ検出手段７０がその機器ＩＤを検出すると、履歴情報とは無関係に、認証手段５０は相手側の認証手段と認証を行う。本実施の形態においては、履歴情報とは無関係に認証を行うので、新たなＡＶデータ送信機器が接続して最初の著作物伝送においても、時間を従来に比較して大幅に短縮できる効果を持つことが明らかである。

【００４６】

【発明の効果】

以上説明したように、本発明は、ユーザから著作物伝送を指示するコマンドを入力した時点から著作物伝送開始までの時間を従来に比較して大幅に短縮できるという効果がある。

【００４７】

その理由は過去に認証を行った履歴がある送受信機器が伝送路に接続すると、ユーザからのコマンド入力が行われる以前に機器認証および鍵交換を行うためである。

【図面の簡単な説明】

【図１】

本発明の第１の実施の形態の著作物保護システムの構成を示すブロック図である。

【図２】

本発明の第１の実施の形態の著作物保護システムの動作状態を示す遷移図である。

【図３】

本発明の第２の実施の形態の著作物保護システムの構成を示すブロック図である。

【図４】

従来の著作物保護システムのブロック図である。

【図５】

従来の著作物保護システムの状態遷移図である。

【符号の説明】

１０、１１　　コマンド入力手段

２０、２１　　コマンド制御手段

３０、３１　　ＡＶデータ送信手段

４０、４１　　暗号化手段

５０、５１、１４０、１４１、２４０　　認証手段

６０、６１、１１０、１１１、２１０　　入出力手段

７０　　機器ＩＤ検出手段

８０　　認証履歴記憶手段

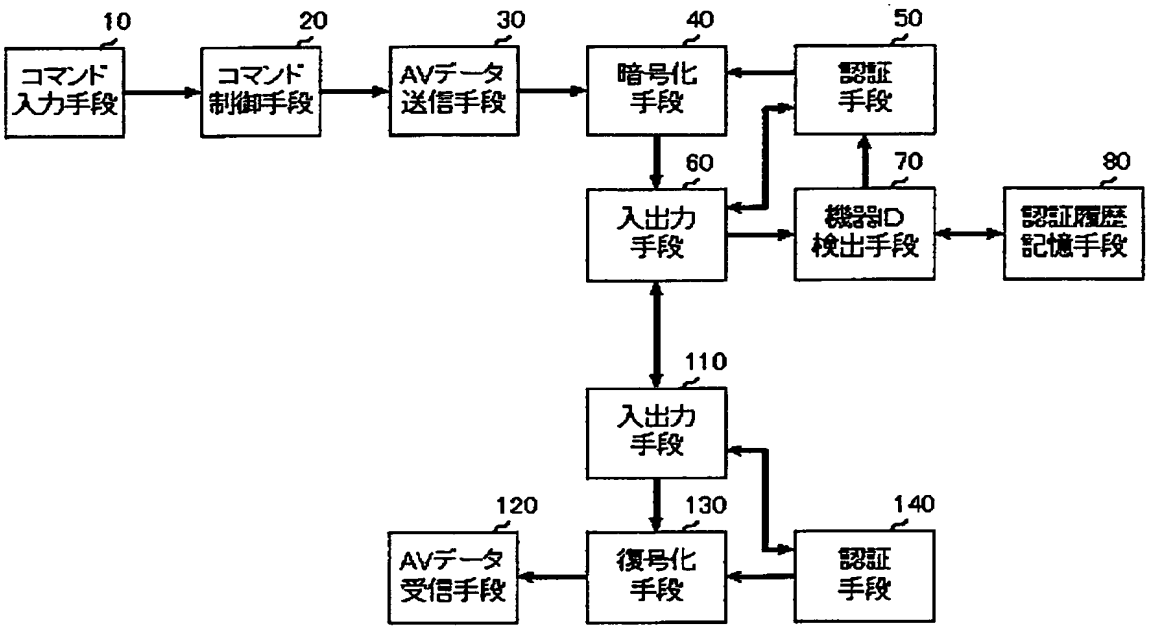
９０　　暗号鍵記憶手段

１２０、１２１、２２０　　ＡＶデータ受信手段

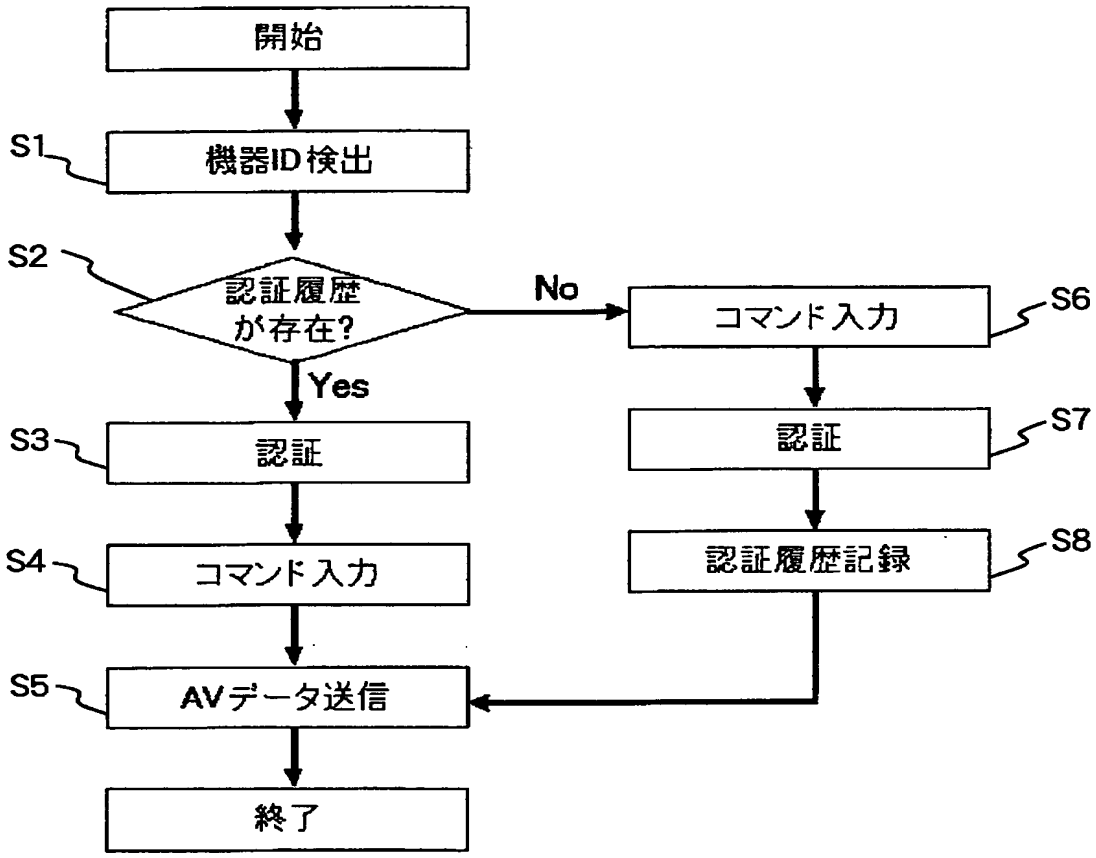
１３０、１３１、２３０　　複号化手段

【書類名】　図面

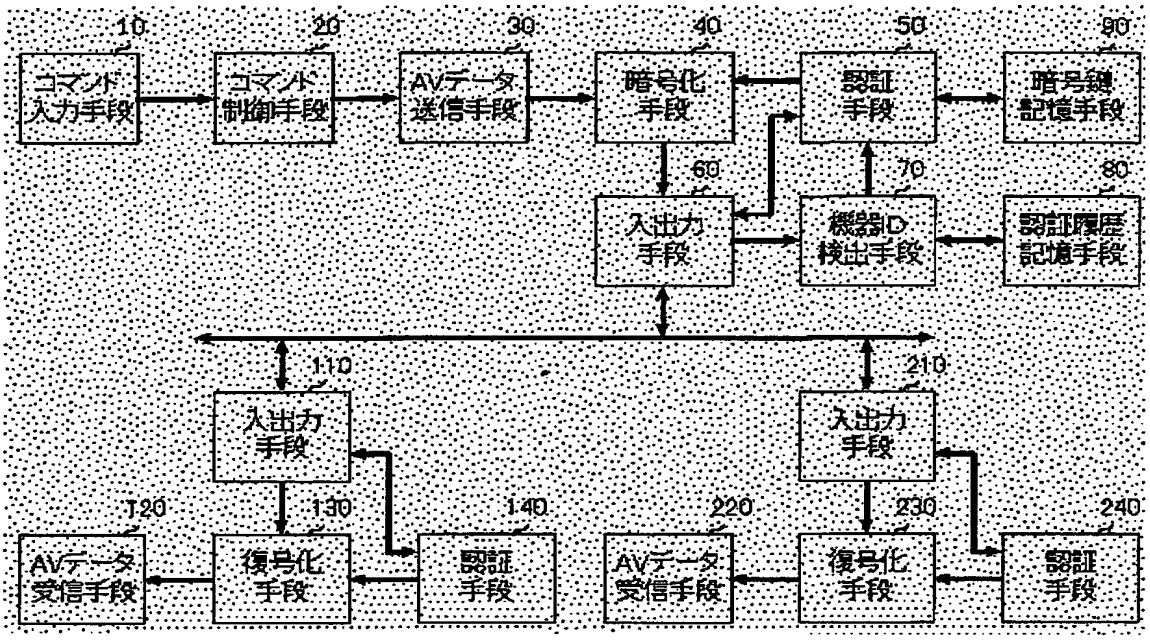
【図１】


10
コマンド入力手段
20
コマンド制御手段
30
AVデータ送信手段
40
暗号化手段
50
認証手段
60
入出力手段
70
機器ID検出手段
80
認証履歴記憶手段
110
入出力手段
120
AVデータ受信手段
130
復号化手段
140
認証手段

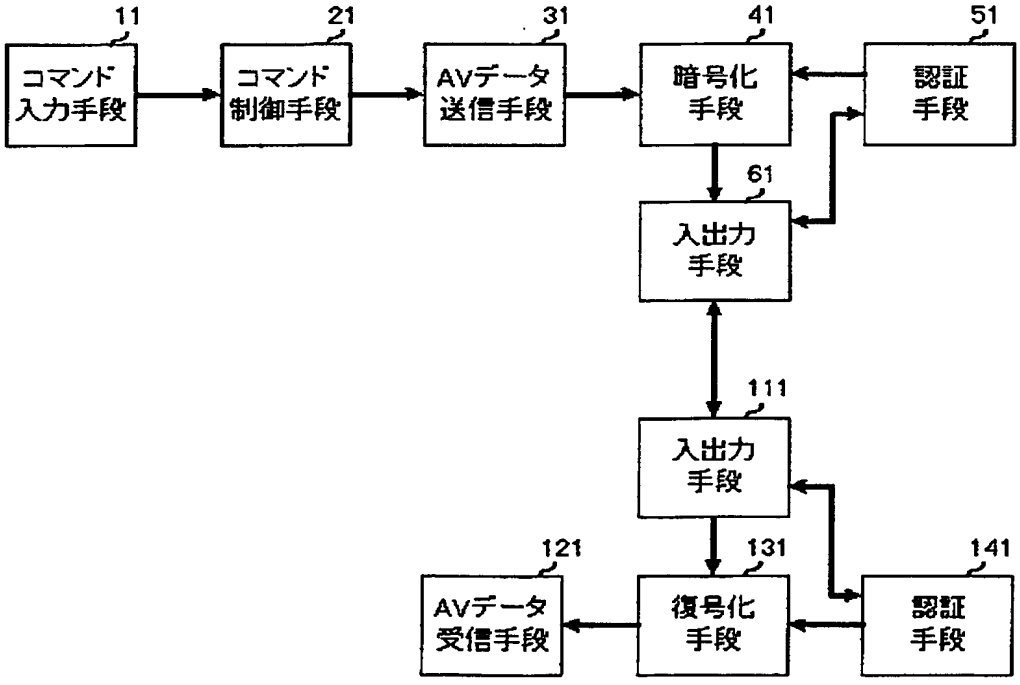
【図２】


開始
S1
機器ID検出
S2
認証履歴
が存在?
No
Yes
S6
コマンド入力
S7
認証
S8
認証履歴記録
S3
認証
S4
コマンド入力
S5
AVデータ送信
終了

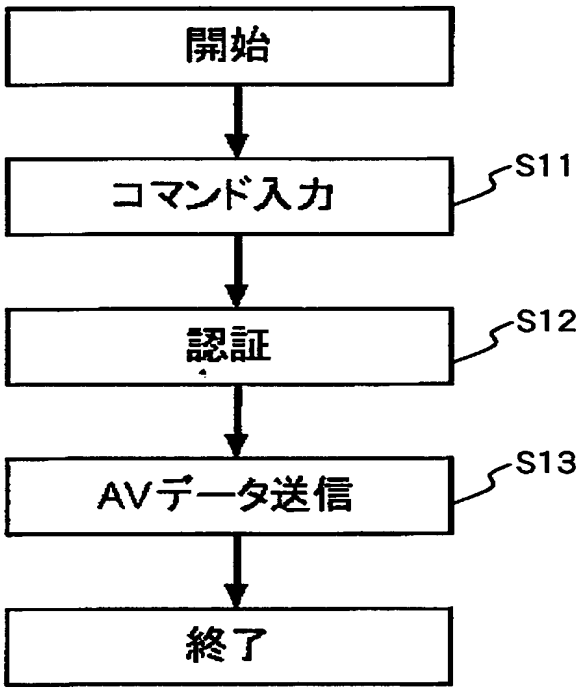
【図３】


10
コマンド入力手段
20
コマンド制御手段
30
AVデータ送信手段
40
暗号化手段
50
認証手段
90
暗号鍵記憶手段
60
入出力手段
70
機器ID検出手段
80
認証履歴記憶手段
110
入出力手段
210
入出力手段
120
AVデータ受信手段
130
復号化手段
140
認証手段
220
AVデータ受信手段
230
復号化手段
240
認証手段

【図４】


11
コマンド入力手段
21
コマンド制御手段
31
AVデータ送信手段
41
暗号化手段
51
認証手段
61
入出力手段
111
入出力手段
121
AVデータ受信手段
131
復号化手段
141
認証手段

【図５】



【書類名】　　要約書

【要約】

【課題】　ＡＶデータ伝送指示からＡＶデータを伝送するまでの時間を短縮する著作物保護システム及びその著作物保護方法を提供することにある。

【解決手段】　機器ＩＤ検出手段７０は相手側の機器ＩＤを検出する。次に、認証履歴記憶手段８０が記憶している履歴情報の中にその機器ＩＤが含まれているかどうかを調べる。もし、履歴情報の中にその機器ＩＤが含まれている場合、認証手段５０は相手側の認証手段１４０と認証を行う。その後、コマンド入力手段１０に対してユーザからＡＶデータ送信指示があると、コマンド制御手段２０を介してＡＶデータ送信手段３０にそのコマンドが通知され、ＡＶデータ送信手段３０はＡＶデータの送信を開始する。

【選択図】　　図１

【書類名】　職権訂正データ
【訂正書類】　特許願

＜認定情報・付加情報＞
【特許出願人】
【識別番号】　000004237
【住所又は居所】　東京都港区芝五丁目７番１号
【氏名又は名称】　日本電気株式会社
【代理人】　申請人
【識別番号】　100070219
【住所又は居所】　東京都港区赤坂１丁目９番２０号　第１６興和ビル８階　若林国際特許事務所
【氏名又は名称】　若林　忠
【選任した代理人】
【識別番号】　100100893
【住所又は居所】　東京都港区赤坂１丁目９番２０号　第１６興和ビル８階
【氏名又は名称】　渡辺　勝
【選任した代理人】
【識別番号】　100088328
【住所又は居所】　東京都港区赤坂１丁目９番２０号　第１６興和ビル８階
【氏名又は名称】　金田　暢之
【選任した代理人】
【識別番号】　100106138
【住所又は居所】　東京都港区赤坂１丁目９番２０号　第１６興和ビル８階
【氏名又は名称】　石橋　政幸
【選任した代理人】
【識別番号】　100106297
【住所又は居所】　東京都港区赤坂１丁目９番２０号　第１６興和ビル８階　若林国際特許事務所
【氏名又は名称】　伊藤　克博

出　願　人　履　歴　情　報

識別番号　　〔０００００４２３７〕

１．変更年月日　　１９９０年　８月２９日
［変更理由］　新規登録
住　所　　東京都港区芝五丁目７番１号
氏　名　　日本電気株式会社